Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

RESEARCH ARTICLE

Reliability analysis of station autonomous computer system based on fuzzy dynamic fault tree and Markov model

Lu Yan[1] | Tao Zhang[2] | Ying Gao[3] | Rongsheng Wang[1,2] | Shuxin Ding[2]

[1]China Academy of Railway Sciences, Beijing 100081, China
[2]Signal and Communication Research Institute, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China
[3]Standards and Metrology Research Institute, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China

Correspondence
Shuxin Ding, Signal and Communication Research Institute, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China.
Email: dingshuxin@rails.cn

Abstract

Station autonomous computer system is the core of the centralized traffic control (CTC) system. The working mode is dual computer hot standby, and its reliability is very important. Due to the dynamic and fuzzy issue with the reliability analysis of station autonomous computer system, a reliability analysis method is formulated based on fuzzy dynamic fault tree (DFT) and Markov model. Firstly, the structure and working principle of the dual computer hot standby autonomous computer system and the double 2-vote-2 autonomous computer system are analyzed, and two autonomous computer systems based on DFT are formulated. Then, the failure rates and the fault detection probabilities are considered as fuzzy variables and represented as triangular fuzzy variables. The fuzzy state transition matrix of the system is obtained by conversion of DFT to the Markov model. Finally, the fuzzy reliability of the system is calculated by Laplace transform. Simulation results show that the reliability of the dual computer hot standby autonomous computer system is higher than that of the double 2-vote-2 autonomous computer system. Besides, the reliability of the hardware system is not only related to the structure of the system, but also affected by the uncertain unit failure rate, fault detection probabilities, etc.

KEYWORDS:
station autonomous computer system, reliability, Markov model, dynamic fault tree, fuzzy set theory

1 | INTRODUCTION

The station autonomous computer system is the special computer system for processing train schedules, executing route control, handling station interfaces information, automatic train tracking, etc., in centralized traffic control (CTC) system. Dual computer hot standby is generally used. When route assignment, route trigger, etc., are implemented in the railway station, it should be confirmed that only one autonomous computer is used at a time; thus uniqueness is ensured for the commands to the controlled object[1]. Therefore, the reliability of the station autonomous computer system and the switching unit for the dual autonomous computer should be confirmed.

Dual computer hot standby means that two computers are used to back up each other and perform the same service together for important services. When the primary module breaks down, the spare unit automatically takes over the tasks without human intervention, which ensures continuous services from the system[1]. In terms of reliability, dual computer hot standby system has incomparable advantages over the single-machine system, and is widely applied in many fields, e.g., industry, agriculture, transportation, information, etc[2,3,4,5,6].

System reliability measures the ability or probability of the system to complete the specified function within the specified time and under the specified working conditions. With the rapid progress of science and technology, the composition of the system becomes more complex, which brings a lot of problems related to reliability. Therefore, an efficient analysis to evaluate the behaviour of complex systems is necessary. Fault tree and Markov models are then commonly used methods for reliability analysis[7,8]. Fault tree analysis uses the graphical representation to describe the logical relationship between top and lower-level events. It is intuitive and logical, but the disadvantage is that it is difficult to model the dynamic random fault effectively[9]. The reliability model established by the Markov model using system state and the state transition can comprehensively describe the dynamic actions. However, the number of states in the Markov model increases exponentially as the number of basic events increase, which makes the model difficult to solve[10]. Therefore, based on the two advantages above, the Markov chain's reliability model is constructed by the dynamic fault tree (DFT), and it has recently become a research hotspot for reliability modeling and analysis of complex systems[11,12].

In order to introduce the Markov chain into reliability modeling in the station autonomous computer system, the component failure rates, and the fault detection probabilities should be considered first. However, because of imprecise measurements, personal judgments, etc., these parameters in the station autonomous computer system tend to have strong ambiguity. In order to deal with the dynamic and fuzzy issue of the station autonomous computer system, a reliability analysis method is formulated based on the fuzzy DFT and the Markov model. The method quantitatively measures the reliability of the station autonomous computer system with different structures. We summarize our contributions as follows:

1. The reliability models of station autonomous computer system with two types: the dual computer hot standby autonomous computer system and the double 2-vote-2 autonomous computer system are proposed and compared.
2. The fuzzy dynamic fault tree is used to describe the system reliability models by conversion to the Markov models.

The rest of the paper is organized as follows. The related works are given in Section 2. In Section 3, the structure of the station autonomous computer system is analyzed. Section 4 describes the technical background of the fuzzy dynamic fault tree. The reliability modeling of the station autonomous computer system is proposed in Section 5. Section 6 shows the obtained case studies. Section 7 gives the conclusions and future works.

2 | RELATED WORKS

In railway transportation, reliability is a very important issue for train operations. Therefore, the redundant structure is often used to improve the reliability of the systems. Hu et al.[13] compared with the application of the traditional turnout driving system and proposed that the hardware redundancy control system would be the direction of the control system in the future. Wang et al.[14] proposed a new strategy of hot standby switching for railway signaling equipment by using synchronization and malfunction comparison. Wang et al.[15] proposed the realizable scheme of the hot standby for CTC based on the basic principle and priority of failover. All of the above works analyzed the systems using qualitative methods.

As for quantitative analysis, Kumar et al.[16] proposed a fault-tolerant and fail-safe node with transputers for a local area network used in distributed railway signaling systems. Kim et al.[17] designed a double 2-vote-2 system based on MC6800 and can be applied to embedded control systems like airplanes and high-speed railway systems. Markov model is also used for reliability analysis. Yan et al.[18] analyzed the reliability of two dual computer hot standby architectures widely used in the railway signaling system using the Markov model. Wen et al.[19] proposed the isomorphic Markov model of dual computer hot standby system with different structures considering the common-cause failure, online diagnosis, and multi-failure modes in the railway signaling system. Liu et al.[20] analyzed the reliability of dual computer hot standby computer-based interlocking control system based on the on-site practical situation. Li et al.[21] established a dynamic fault tree analysis model of the probability of falling danger and probability of falling safety for dual computer hot standby and double 2-vote-2 computer-based interlocking systems.

Generally speaking, the current research on dual computer hot standby in railway systems mainly focused on signal communication and computer-based interlocking systems. There are few works on the station autonomous computer system, especially the structure and reliability analysis of the station autonomous computer system, which is still at the stage of exploration. Besides, the uncertainty of the failure rate for the station autonomous computer system is not considered.

3 | ANALYSIS OF THE STRUCTURE OF STATION AUTONOMOUS COMPUTER SYSTEM

The dual computer hot standby system consists of two identical autonomous computer operation modules and a switching unit. The system adopts dual redundancy to work cooperatively with the external device. Usually, two autonomous computer operation modules work simultaneously: dealing with the same data and accomplishing the same tasks. The switching unit will assign one of the two autonomous computer operation modules as the primary module. When the primary module fails, the other autonomous computer operation module (standby module) will switch to the primary module by the switching signal from the switching unit. Therefore, normal operation is ensured. The structure of the dual computer hot standby autonomous computer system is shown in Fig. 1. Each autonomous computer operation module contains a unique processor, drive, and acquisition control system. The module also has a self-diagnosis function that can detect faults.

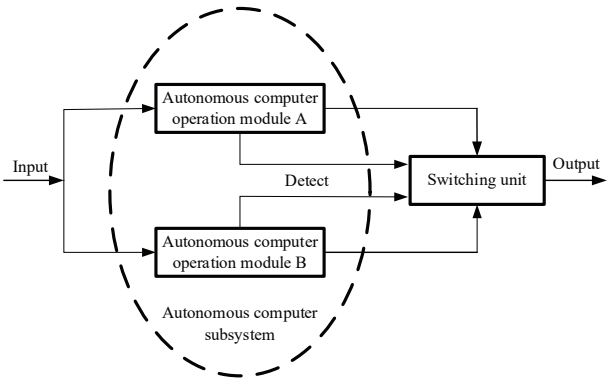


FIGURE 1 The structure of dual computer hot standby autonomous computer system.

The double 2-vote-2 autonomous computer system consists of two comparison subsystems for "double" and two operation modules with the same task in a comparison subsystem for "2-vote-2". Once the operation results of the autonomous computer operation modules are different, the system will give a warning of "error" and refuse to output the instruction information. The double 2-vote-2 autonomous computer system structure is shown in Fig. 2, in which most of the comparators are customized or semi-customized devices with good reliability[22].

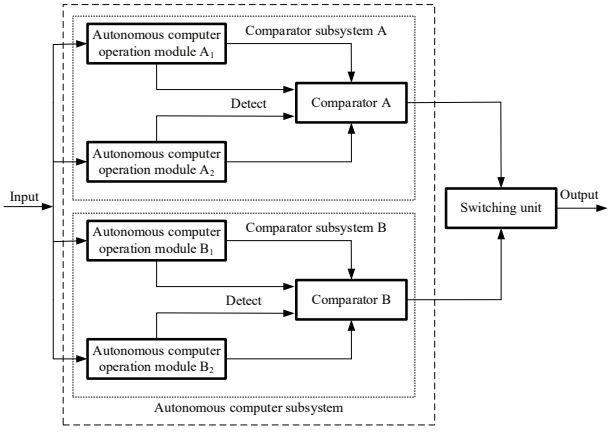
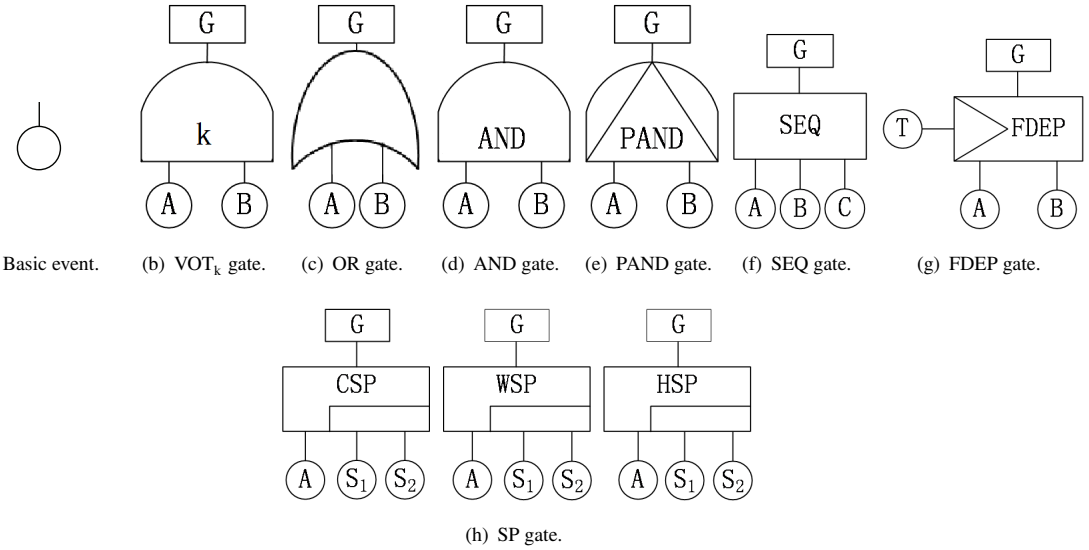


FIGURE 2 The structure of double 2-vote-2 autonomous computer system.

The switching units in Fig. 1 and 2 consist of two separate switching plates and a set of safety mutex relays. It mainly performs communication and hot standby switching between two autonomous computer operation modules or two comparators and channel switching of interface devices. Due to the safety mutex relays, the states of relays collected simultaneously by two



(a) Basic event. (b) VOT_k gate. (c) OR gate. (d) AND gate. (e) PAND gate. (f) SEQ gate. (g) FDEP gate.

(h) SP gate.

FIGURE 3 Node types in ((a)–(d)) static and (all) dynamic fault trees.

autonomous computer operation modules or two comparators must be mutually exclusive, which avoids two primary modules as a result.

We have the following assumptions for analyzing the system:

1. The failure rates and fault detection probabilities of the operation module belong to the same fuzzy variables, λ and c, respectively.
2. All the operation modules are at the normal state at the beginning.
3. We do not fix the system after its failure.
4. We consider that the switching units and the comparators have good reliability.

4 | TECHNICAL BACKGROUND

4.1 | Basic events and gates for static fault trees

Fault trees are directed acyclic graphs with different types of nodes (AND, OR, etc.)[23]. Nodes without children are basic events (BEs, Fig. 3(a)). Each BE may fail according to the failure rate. A fault tree consists of BEs and gates. A gate fails if its children hold the failure condition.

In static fault trees (SFTs), the voting gate (VOT_k) denotes that it fails if more than its k children have failed. As a result, a VOT_1 gate equals an OR gate, and a VOT_k gate with k children equals an AND gate.

4.2 | Dynamic fault trees and dynamic gates

The fault-tree model in the traditional fault-tree analysis cannot capture the sequence dependencies in the system[7,24]. Dynamic fault tree (DTF) extends the traditional one by adding four dynamic gates, which are the priority AND (PAND) gate, the sequence enforcing (SEQ) gate, the functional dependency (FDEP) gate, and the spare (SP) gate[24,25,26].

PAND gate

PAND gate (Fig. 3(e)) extends the AND gate by an additional condition. For an output event (G) and two input events (A and B), G occurs only when both A and B occur, and A occurs before B.

SEQ gate

SEQ gate (Fig. 3(f)) consists of several input events (A, B, and C) and an output event (G). Other than the PAND gate, the SEQ gate forces its inputs to fail based on a particular order[10]: G occurs only when A, B, and C occur in order.

FDEP gate

FDEP gate (Fig. 3(g)) consists of one trigger-input event (T), one independent output event (G), and several dependent events (A, B). When T occurs, the output event occurs, and the dependent events are forced to occur. Besides, the occurrence of any dependent events does not affect the trigger event[10].

SP gate

SP gate (Fig. 3(h)) consists of an output event (G), a primary module (A), and several standby modules (spares). When a primary module (component) A fails, it can be substituted by spares S1 and S2. In other words, event G occurs when A, S1, and S2 fail. According to the switching relationship of the primary and standby modules, the SP gate can be divided into three types: cold spare gate (CSP), warm spare gate (WSP), and hot spare gate (HSP)[27].

As a supplement for the primary module in a CSP, the standby modules are not powered until they replace the primary modules when a fault occurs. However, in a WSP, the standby modules are powered initially (warm standby state) with a failure rate. The failure rate is less or equal to that when a faulty module is replaced. In an HSP, it is a special case compared to WSP that the failure rate of a standby module remains the same in the warm standby state and working state[27].

4.3 | The conversion of dynamic gates to Markov model

To calculate the reliability of the system, the dynamic gates could be converted to the corresponding continuous time Markov chain[24,28,29,30]. That is, consider possible combinations of input events as basic states of the Markov model, and use the failure rate as the state transition rate of the Markov model. Then, we can calculate the reliability curves.

The conversion of PAND gate

Fig. 4 shows the conversion of the PAND gate, where "00" denotes the normal states of the input modules A and B. "10" denotes that A fails and B continues to work. "01" denotes that modules B fails and A continues to work. "11" denotes that both modules A and B fail. "Fa" denotes that the output event G occurs and the system fails. λ_A and λ_B denote the failure rate of the modules A and B. "Fa" occurs only when the transition state "00" to "10" and "10" to "Fa".

The conversion of SEQ gate

Fig. 5 shows the conversion of SEQ gate, where λ_C denotes the failure rate of input module C. "000" denotes the input modules A, B, and C are in normal states. The meaning of the other states is similar to Fig. 4.

The conversion of FDEP gate

Fig. 6 shows the conversion of the FDEP gate, where λ_T denotes the failure rate of rigger-input event T. "000" denotes the input modules T, A, and B are in normal states. The meaning of the other states is similar to Fig. 4.

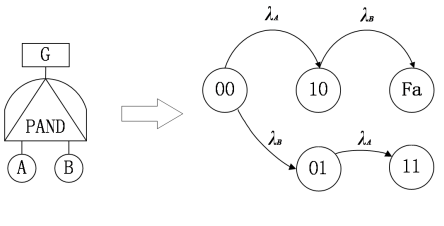


FIGURE 4 PAND conversion to Markov model.

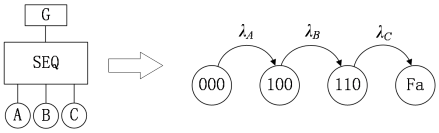


FIGURE 5 SEQ conversion to Markov model.

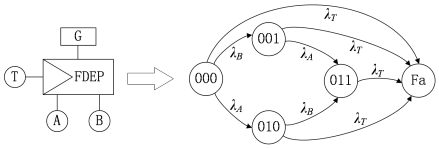
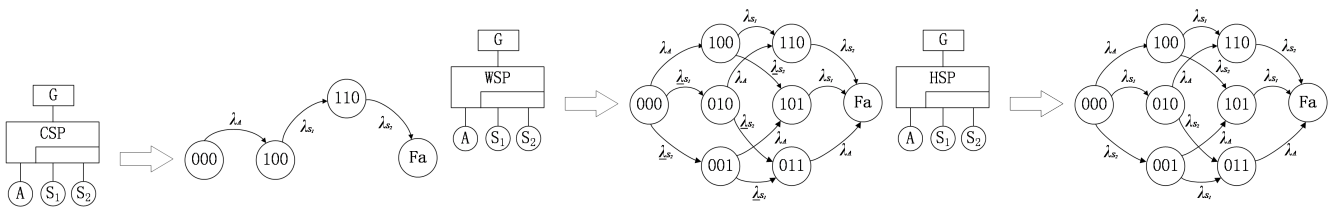


FIGURE 6 FDEP conversion to Markov model.

The conversion of SP gate

Fig. 7 shows the conversion of SP gate, where λ_{s_1}, λ_{s_2}, $\underline{\lambda}_{s_1}$, and $\underline{\lambda}_{s_2}$ denote the failure rate of standby modules S1, S2, and the failure rate of standby modules S1, S2 before primary module A fails, respectively. $\underline{\lambda}_{s_1} = \alpha\lambda_{s_1} < \lambda_{s_1}$ and $\underline{\lambda}_{s_2} = \alpha\lambda_{s_2} < \lambda_{s_2}$ $(0 \leq \alpha \leq 1)$ denote that the failure rate of standby modules S1 and S2 before primary module A fails, respectively. $\underline{\lambda}_{s_1} = \lambda_{s_1}$ and $\underline{\lambda}_{s_2} = \lambda_{s_2}$ denote that S1 and S2 are switched powered ones (HSP gate, $\alpha = 1$). For CSP gate, $\alpha = 0$.



(a) CSP conversion to Markov model. (b) WSP conversion to Markov model. (c) HSP conversion to Markov model.

FIGURE 7 SP conversion to Markov model.

4.4 | Fuzzy set

Zadeh proposed the fuzzy set theory to deal with the uncertainty in engineering projects[31,32]. Suppose that a fuzzy subset A in a universe of discourse U. For any $u \in U$, the membership degree is determined by the corresponding real number $\mu_A(u) \in [0, 1]$. A is the fuzzy subset, and $\mu_A(u)$ is the membership degree of u to A.

If the fuzzy subset A is convex, A is called the fuzzy variable. There are three commonly used fuzzy variables: Gaussian fuzzy variables, triangular fuzzy variables, and trapezoidal fuzzy variables. Fig. 8 shows the triangular fuzzy variables, whose membership function is described as follows:

$$\mu_A(x) = \begin{cases} \frac{x-a}{b-a} & a \leq x < b \\ 1 & x = b \\ \frac{x-c}{b-c} & b \leq x < c \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

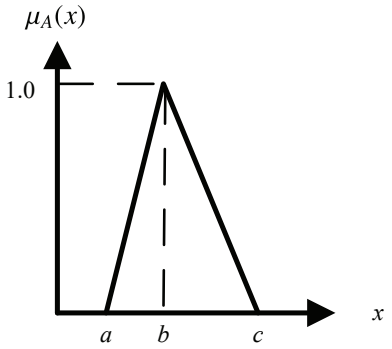


FIGURE 8 The membership function of triangular fuzzy variables.

5 | RELIABILITY MODELING OF STATION AUTONOMOUS COMPUTER SYSTEM

5.1 | System reliability modeling based on Markov model and DFT

Suppose that the failure rates and the fault detection probabilities are considered as triangular fuzzy variables, denoted by $\tilde{\lambda}(q_1, \lambda, q_2)$ and $\tilde{c}(q_3, c, q_4)$. The lower and upper bounds of the dispersion region of $\tilde{\lambda}$ and $\tilde{c}$ are q_1, q_2 and q_3, q_4, respectively. These values can be obtained by fuzziness, experience and statistical data from real applications.

The DFT model is established based on the failure analysis on the CTC system, and the DFT with n states is converted by adopting the Markov model. The fuzzy parameters in the converted Markov model are the transition probabilities, and the fuzzy state transition matrix is as follows:

$$\tilde{\mathbf{A}} = \left(\tilde{\lambda}_{i,j}\right) = \begin{pmatrix} \tilde{\lambda}_{1,1} & \tilde{\lambda}_{1,2} & \cdots & \tilde{\lambda}_{1,n} \\ \tilde{\lambda}_{2,1} & \tilde{\lambda}_{2,2} & \cdots & \tilde{\lambda}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{\lambda}_{n,1} & \tilde{\lambda}_{n,2} & \cdots & \tilde{\lambda}_{n,n} \end{pmatrix} \tag{2}$$

The transition process of the system fuzzy states is shown in Fig. 9, where S_1 denotes that system is in good condition, $S_i (i = 2, \cdots, n-1)$ denotes an intermediate state that some of the components fail in the system. However, the system still works normally, and S_n denotes that the system is in a failure state.

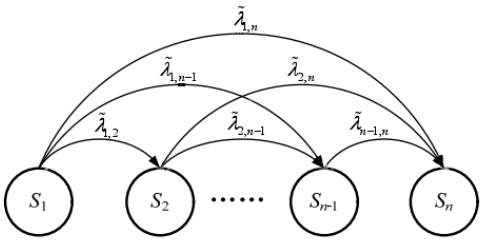


FIGURE 9 The fuzzy state transition diagram of a system.

The corresponding differential equations in Fig. 9 is calculated as

$$\begin{cases} \tilde{p}_1'(t) = -\tilde{p}_1(t) \sum_{j=2}^{n} \tilde{\lambda}_{1,j} \\ \tilde{p}_i'(t) = \sum_{j=1}^{i-1} \tilde{p}_j(t)\tilde{\lambda}_{j,i} - \sum_{j=i+1}^{n} \tilde{p}_i(t)\tilde{\lambda}_{i,j} \quad 1 < i < n \\ \tilde{p}_n'(t) = \sum_{j=1}^{n-1} \tilde{p}_j(t)\tilde{\lambda}_{j,n} \end{cases} \tag{3}$$

Take the Laplace transform of Eq. (3) with the initial condition $\tilde{p}_1(0) = 1$ and $\tilde{p}_i(0) = 0$ $(i \neq 1)$, we have the following:

$$\begin{cases} s\tilde{p}_1(s) - 1 = -\tilde{p}_1(s) \sum_{i=2}^{n} \tilde{\lambda}_{1,i} \\ s\tilde{p}_i(s) = \sum_{j=1}^{i-1} \tilde{p}_j(s)\tilde{\lambda}_{j,i} - \sum_{j=i+1}^{n} \tilde{p}_i(s)\tilde{\lambda}_{i,j} \quad 1 < i < n \\ s\tilde{p}_n(s) = \sum_{j=1}^{n-1} \tilde{p}_j(s)\tilde{\lambda}_{j,n} \end{cases} \tag{4}$$

A function of s named $\tilde{p}_n(s)$ is obtained by solving the above equations and taking the inverse Laplace transform, the probability distribution $\tilde{p}_n(t)$ in terms of time can be obtained.

The upper and lower bounds of the fuzzy variables $\tilde{p}_n(t)$, which is the fuzzy failure rate of the CTC system, can be calculated by the failure rates and the fault detection probabilities under different membership degree.

5.2 | Reliability modeling of dual computer hot standby autonomous computer system

Suppose that the operation modules A and B in Fig. 1 are the primary and standby modules. Through the reliability analysis of dual computer hot standby system with the failure rate λ and the fault detection probability c, the system will appear fail-safe state and hazard output state, and the dynamic fault tree model of the system is obtained, shown in Fig. 10.

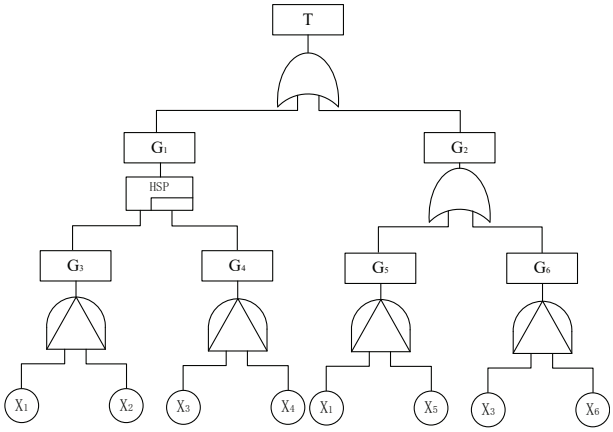


FIGURE 10 The dynamic fault tree of dual computer hot standby autonomous computer system.

In Fig. 10, T denotes that system fails, G_1 denotes the system fail-safe state, G_2 denotes that the system is in hazard output state. G_3 and G_4 denotes the fail-safe state of operation modules A and B, respectively. G_5 denotes the hazard output of operation module A, which leads the system's hazard output. G_6 denotes a detected failure in module A, switches to module B, and the hazard output of module B, leading to the system's hazard output. X_1 and X_3 denote failure in modules A and B, respectively. X_2 and X_4 denote that modules A and B have been detected, respectively. X_5 and X_6 denote that modules A and B have not been detected, respectively.

The meaning of the dynamic gates in Fig. 10 is as follows. The HSP gate denotes operation modules A and B are both in the fail-safe output state, and the system is in the fail-safe output state. There are four PAND gates: 1, 2, 3, and 4 from left to right. The PAND gate 1/2 denotes the fail-safe output when A/B fails and is detected. The PAND gate 3 denotes a failure in module A, and the system switches to the hazard output state. The PAND gate 4 denotes a detected failure in module A and switches to module B. However, an undetected failure in module B leads to the hazard output state.

Based on the above analysis, the system reliability is calculated by:

$$R(t) = 1 - P(T) \tag{5}$$

We can transform the failure rate λ and the fault detection probability c into triangular fuzzy variables, and conduct further reliability analysis of the DFT in Fig. 10. The Markov model based on the DFT is shown in Fig. 11, where S_1 denotes normal state, S_2 denotes a detected failure in only one operation module, S_3 denotes the working module is in the normal state. In contrast, the standby module exists an undetected failure, and S_4 denotes system failure.

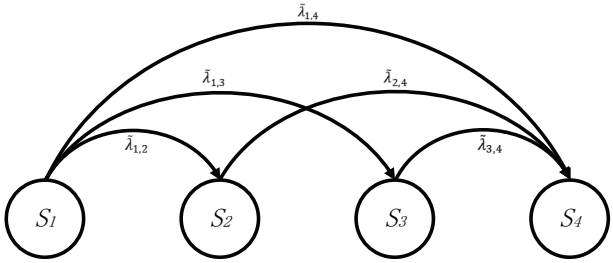


FIGURE 11 The state transition diagram of dual computer hot standby autonomous computer system.

The system's fuzzy state transition matrix is obtained by synthesizing the state transition diagram and fuzzy parameter variables and calculated as follows.

$$\tilde{A} = \begin{pmatrix} -2\tilde{\lambda} & 2\tilde{\lambda}\tilde{c} & \tilde{\lambda}(1-\tilde{c}) & \tilde{\lambda}\left(1-\widetilde{c}\right) \\ 0 & -\tilde{\lambda} & 0 & \tilde{\lambda} \\ 0 & 0 & -\tilde{\lambda} & \tilde{\lambda} \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{6}$$

The corresponding differential equations of the state transition diagram is calculated as

$$\begin{cases} \tilde{p}_1'(t) = -\tilde{p}_1(t)2\tilde{\lambda} \\ \tilde{p}_2'(t) = 2\tilde{p}_1(t)\tilde{\lambda}\tilde{c} - \tilde{p}_2(t)\tilde{\lambda} \\ \tilde{p}_3'(t) = \tilde{p}_1(t)\tilde{\lambda}(1-\tilde{c}) - \tilde{p}_3(t)\tilde{\lambda} \\ \tilde{p}_4'(t) = \tilde{p}_1(t)\tilde{\lambda}(1-\tilde{c}) + \tilde{p}_2(t)\tilde{\lambda} + \tilde{p}_3(t)\tilde{\lambda} \end{cases} \tag{7}$$

Take the Laplace transform of Eq. (7) with the initial condition $\tilde{p}_1(0) = 1$ and $\tilde{p}_i(0) = 0$ $(i \neq 1)$, we have the following:

$$\begin{cases} s\tilde{p}_1(s) - 1 = -\tilde{p}_1(s)2\tilde{\lambda} \\ s\tilde{p}_2(s) = 2\tilde{p}_1(s)\lambda\tilde{c} - \tilde{p}_2(s)\tilde{\lambda} \\ s\tilde{p}_3(s) = \tilde{p}_1(s)\tilde{\lambda}(1-\tilde{c}) - \tilde{p}_3(s)\tilde{\lambda} \\ s\tilde{p}_4(s) = \tilde{p}_1(s)\tilde{\lambda}(1-\tilde{c}) + \tilde{p}_2(s)\tilde{\lambda} + \tilde{p}_3(s)\tilde{\lambda} \end{cases} \tag{8}$$

A function of s named $\tilde{p}_4(s)$ is obtained by solving the above equation, that is,

$$\tilde{p}_4(s) = \frac{\tilde{\lambda}(1-\tilde{c})(s+\tilde{\lambda}) + 2\tilde{c}\tilde{\lambda}^2 + \tilde{\lambda}^2(1-\tilde{c})}{s(s+2\tilde{\lambda})(s+\tilde{\lambda}))} \tag{9}$$

Taking the inverse Laplace transform, the probability of S_4 is calculated as follows.

$$\tilde{P}_4(t) = ce^{-2\tilde{\lambda}t} - (1+c)e^{-\tilde{\lambda}t} + 1 \tag{10}$$

It is a function with respect to time t, which in fact is also the fuzzy failure probability function of the system.

5.3 | Reliability modeling of double 2-vote-2 autonomous computer system

Suppose that the subsystems A and B in Fig. 2 are the primary and standby modules. Through the reliability analysis of the double 2-vote-2 system with the failure rate λ and the fault detection probability c. The system will appear fail-safe state and hazard output state, and the dynamic fault tree model of the system is obtained, shown in Fig. 12.

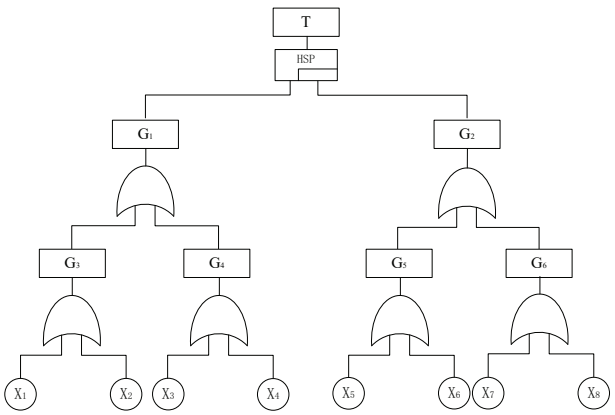


FIGURE 12 The dynamic fault tree of double 2-vote-2 autonomous computer system.

In Fig. 12, T denotes that system fails, G_1 and G_2 denotes the fail-safe state of subsystem A and B, respectively. G_3 and G_5 denote detected failures in the operation modules, which leads to the output of fail-safe state, respectively. G_4 and G_6 denote the comparators A and B detects the inconsistency between the results of the two operation modules, and the corresponding subsystem fails and is removed, respectively. X_1, X_2, X_5, and X_6 denote the detected failure in operation modules A_1, A_2, B_1, and B_2, respectively. X_3, X_4, X_7, and X_8 denote the undetected failure in operation modules A_1, A_2, B_1, and B_2 respectively.

The meaning of the dynamic gates in Fig. 12 is as follows. The HSP gate denotes A and B are both in a fail-safe output state, and the system is in a fail-safe output state. The system reliability is also calculated by Eq. (5).

We can transform the failure rate λ and the fault detection probability c into triangular fuzzy variables, and conduct further reliability analysis of the DFT in Fig. 12. The Markov model based on the DFT is shown in Fig. 13, where S_1 denotes a normal state in the four operation modules, S_2 denotes a detectable failure in one operation module of a subsystem, S_3 denotes an undetectable failure in one operation module of a subsystem, S_4 denotes that both of the operation modules fail in a subsystem, and S_5 denotes system failure where both subsystems fail.

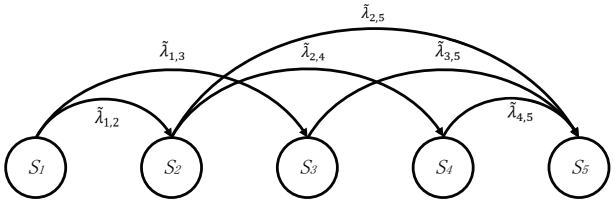


FIGURE 13 The state transition diagram of double 2-vote-2 autonomous computer system.

The fuzzy state transition matrix of the system is obtained by synthesizing the state transition diagram and fuzzy parameter variables, and is calculated as follows.

$$\tilde{A} = \begin{pmatrix} -4\tilde{\lambda} & 4\tilde{\lambda}\tilde{c} & 4\tilde{\lambda}(1-\tilde{c}) & 0 & 0 \\ 0 & -3\tilde{\lambda} & 0 & \tilde{\lambda} & 2\tilde{\lambda} \\ 0 & 0 & -2\tilde{\lambda} & 0 & 2\tilde{\lambda} \\ 0 & 0 & 0 & -2\tilde{\lambda} & 2\tilde{\lambda} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{11}$$

The corresponding differential equations of the state transition diagram is calculated as

$$\begin{cases} \tilde{p}_1'(t) = -\tilde{p}_1(t)4\tilde{\lambda} \\ \tilde{p}_2'(t) = 4\tilde{p}_1(t)\tilde{\lambda}\tilde{c} - 3\tilde{p}_2(t)\tilde{\lambda} \\ \tilde{p}_3'(t) = 4\tilde{p}_1(t)\tilde{\lambda}(1-\tilde{c}) - 2\tilde{p}_3(t)\tilde{\lambda} \\ \tilde{p}_4'(t) = \tilde{p}_2(t)\tilde{\lambda} - 2\tilde{p}_4(t)\tilde{\lambda} \\ \tilde{p}_5'(t) = 2\tilde{p}_2(t)\tilde{\lambda} + 2\tilde{p}_3(t)\tilde{\lambda} + 2\tilde{p}_4(t)\tilde{\lambda} \end{cases} \tag{12}$$

Take the Laplace transform of Eq. (12) with the initial condition $\tilde{p}_1(0) = 1$ and $\tilde{p}_i(0) = 0$ $(i \neq 1)$, we have the following:

$$\begin{cases} s\tilde{p}_1(s) - 1 = -\tilde{p}_1(s)4\tilde{\lambda} \\ s\tilde{p}_2(s) = 4\tilde{p}_1(s)\tilde{\lambda}\tilde{c} - 3\tilde{p}_2(s)\tilde{\lambda} \\ s\tilde{p}_3(s) = 4\tilde{p}_1(s)\tilde{\lambda}(1-\tilde{c}) - 2\tilde{p}_3(s)\tilde{\lambda} \\ s\tilde{p}_4(s) = \tilde{p}_2(s)\tilde{\lambda} - 2\tilde{p}_4(s)\tilde{\lambda} \\ s\tilde{p}_5(s) = 2\tilde{p}_2(s)\tilde{\lambda} + 2\tilde{p}_3(s)\tilde{\lambda} + 2\tilde{p}_4(s)\tilde{\lambda} \end{cases} \tag{13}$$

A function of s named $\tilde{p}_5(s)$ is obtained by solving the above equation, that is,

$$\tilde{p}_5(s) = \frac{8\tilde{\lambda}^2\tilde{c}(s+2\tilde{\lambda}) + 8\tilde{c}\lambda^3 + 8\tilde{\lambda}^2(1-\tilde{c})(s+3\tilde{\lambda})}{s(s+3\tilde{\lambda})(s+2\tilde{\lambda})(s+4\tilde{\lambda})} \tag{14}$$

Taking the inverse Laplace transform, the probability of S_5 is calculated as follows.

$$\tilde{P}_5(t) = 1 - 2e^{-2\tilde{\lambda}t} + e^{-4\tilde{\lambda}t} \tag{15}$$

6 | CASE STUDIES

In this section, the case studies of fuzzy dynamic fault tree on the station autonomous computer system are given. Suppose that the failure rate and the fault detection probability of an operation module are both triangular fuzzy variables. We set 6 instances shown in Table 1 with different fuzzy failure rates and fuzzy fault detection probability.

TABLE 1 Fuzzy failure rate and fault detection probability of the operation module in different cases

Instance	Fuzzy failure rate $\lambda \times 10^{-2}/h$	Fuzzy fault detection probability c
Case 1	(0.09, 0.1, 0.11)	(0.89, 0.9, 0.91)
Case 2	(0.009, 0.01, 0.011)	(0.89, 0.9, 0.91)
Case 3	(0.09, 0.1, 0.11)	(0.69, 0.7, 0.71)
Case 4	(0.009, 0.01, 0.011)	(0.69, 0.7, 0.71)
Case 5	(0.09, 0.1, 0.11)	(0.49, 0.5, 0.51)
Case 6	(0.009, 0.01, 0.011)	(0.49, 0.5, 0.51)

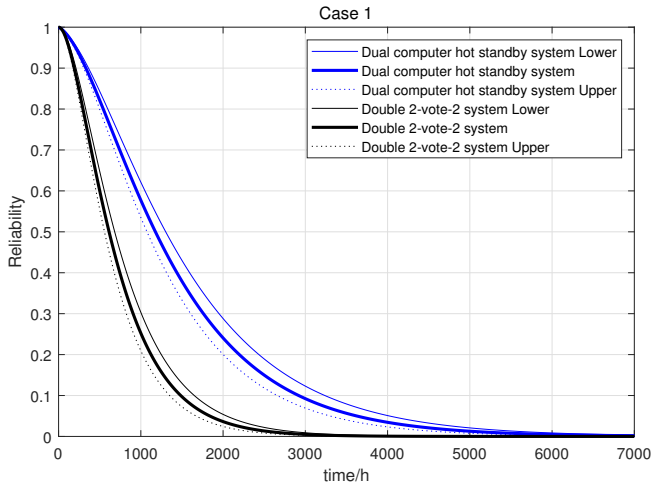
The fuzzy reliability of the station autonomous computer system on different cases is shown in Fig. 14. Due to the difference in fuzzy failure rate with different cases, we set the time interval for cases 1, 3, 5 as [0,7000], and for cases 2, 4, 6 as [0,70000]. The curves of the probability for the dual computer hot standby system and the double 2-vote-2 system are computed based on Eqs. (5), (10), and (15). The lower and upper bound of the system reliability is computed according to the lower and upper bound of the fuzzy failure rates and the fuzzy fault detection probabilities.

We find that among all the cases, the dual computer hot standby system's reliability is higher than that of the double 2-vote-2 system. It may be affected by the number of the operation modules used in the systems, since there are more operation modules in the double 2-vote-2 system. Besides, we find that among cases with the same fuzzy failure rate λ (e.g., cases 1, 3, and 5 or cases 2, 4, and 6), the dual computer hot standby system's reliability increases with the fault detection probability c. However, the double 2-vote-2 system's reliability is not affected by the fault detection probability. It can be confirmed by Eq. (15), where the fault detection probability is not related. Meanwhile, the system reliability increases when the fuzzy failure rate decreases (e.g., between cases 1 and 2, or cases 3 and 4, or cases 5 and 6).

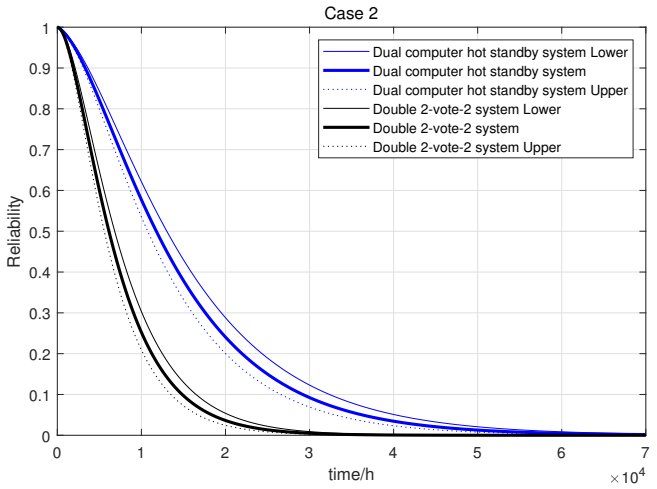
7 | CONCLUSION

To deal with the dynamic and fuzzy issue in the reliability analysis of the station autonomous computer system, a reliability analysis method is proposed based on fuzzy DFT and Markov model. First, two autonomous computer systems based on DFT are formulated. Then, the failure rates and the fault detection probabilities are transformed to triangular fuzzy variables. The fuzzy state transition matrix of the system is obtained by the Markov model. Finally, the fuzzy reliability of the system with given time is calculated by Laplace transform. Case studies show that the dual computer hot standby system's reliability is higher than that of the double 2-vote-2 system. Meanwhile, the hardware system's reliability is related to the structure of the system and affected by the uncertain failure rate, fault detection probabilities, etc.

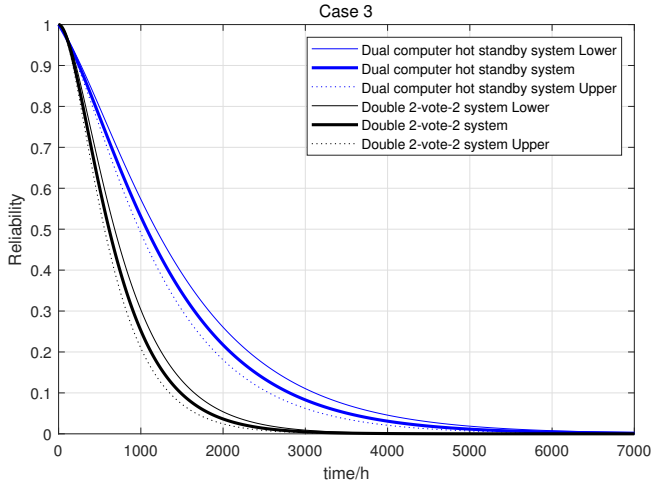
In the future, we will consider the stochastic computation models of the failure rates and the fault detection probabilities.



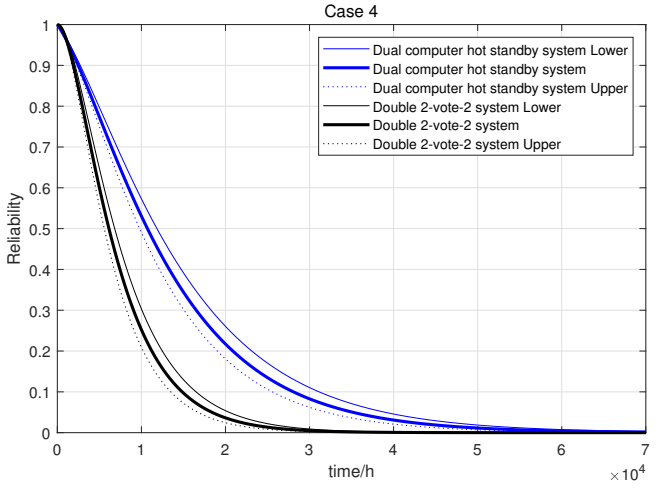
(a) Case 1.



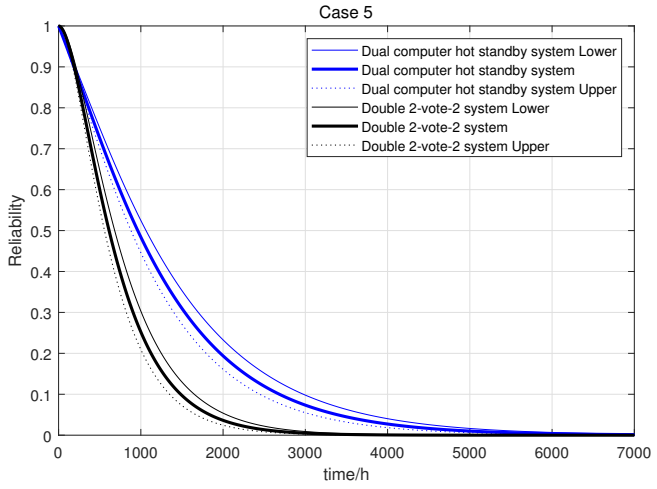
(b) Case 2.



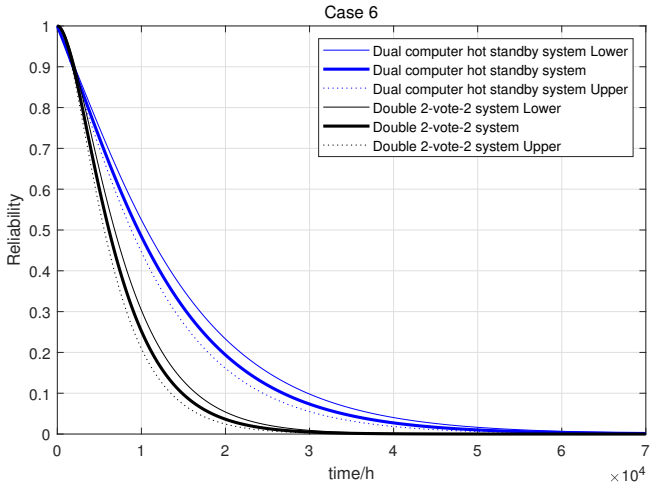
(c) Case 3.



(d) Case 4.



(e) Case 5.



(f) Case 6.

FIGURE 14 Fuzzy reliability comparison of the two systems.

ACKNOWLEDGMENTS

The authors would like to thank the editors and anonymous reviewers for their helpful comments and suggestions on improving the presentation of this paper. This work was supported in part by the National Natural Science Foundation of China under grant U1834211 and U1934220.

Conflict of interest

The authors declare no potential conflict of interests.

References

1. Chen X, Wang Z. The design and implementation of the double hot standby machine of autonomous machine. *Railw. Signal. Commun. Eng.* 2015; 12(4): 86–87.
2. Samet R. Recovery device for real-time dual-redundant computer systems. *IEEE Trans. Dependable Secur. Comput.* 2010; 8(3): 391–403.
3. Sun G, Zhang L, Yibo X. Straw resource mass storage system's design and implementation. *J. Comput. Res. Dev.* 2011; 48(Suppl.): 78–83.
4. Park K, Kim S. Availability analysis and improvement of active/standby cluster systems using software rejuvenation. *J. Syst. Softw.* 2002; 61(2): 121–128.
5. Mukherjee A, Dhar AS. Real-time fault-tolerance with hot-standby topology for conditional sum adder. *Microelectron. Reliab.* 2015; 55(3-4): 704–712.
6. Levitin G, Xing L, Dai Y. Cold vs. hot standby mission operation cost minimization for 1-out-of-N systems. *Eur. J. Oper. Res.* 2014; 234(1): 155–162.
7. Dugan JB, Bavuso SJ, Boyd MA. Fault trees and sequence dependencies. In: Annu. Proc. Reliab. Maintainab. Symp. IEEE. ; 1990: 286–293.
8. Meshkat L, Dugan JB, Andrews JD. Dependability analysis of systems with on-demand and active failure modes, using dynamic fault trees. *IEEE Trans. Reliab.* 2002; 51(2): 240–251.
9. Liu D, Zhang H, Wang B. *Methodologies of dynamic fault trees analysis*. National Defense Industry Press . 2013.
10. Rao KD, Gopika V, Rao VVSS, Kushwaha HS, Verma AK, Srividya A. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. *Reliab. Eng. Syst. Saf.* 2009; 94(4): 872–883.
11. Yevkin O. An efficient approximate Markov chain method in dynamic fault tree analysis. *Qual. Reliab. Engng. Int.* 2016; 32(4): 1509–1520.
12. Aslansefat K, Latif-Shabgahi GR. A hierarchical approach for dynamic fault trees solution through semi-Markov process. *IEEE Trans. Reliab.* 2020; 69(3): 986–1003.
13. Hu A, Yang Y. Design and research on the electric control system for turnout of urban mass transit in Chongqing. *J. Railw. Eng. Soc.* 2009(11): 73–75,80.
14. Wang J, Li Z, Zhao L. Research of active-standby switch in dual machine hot-standby system. *Railw. Signal. Commun.* 2015; 54(2): 11–12.
15. Wang X. Research and realization of hot standby for centralized traffic control system. *J. Beijing Jiaotong Univ.* 2009; 33(2): 26–29.
16. Kumar KV, Chandra V. Transputer-based fault-tolerant and fail-safe node for dual ring distributed railway signalling systems. *Microprocess. Microsyst.* 1994; 18(3): 141–150.
17. Kim H, Lee J, Lee K, Lee H. Design of dual-duplex system and evaluation of RAM. In: ITSC 2001. 2001 IEEE Intell. Transp. Syst. Proc. (Cat. No.01TH8585). IEEE. ; 2001: 710–715.
18. Yan J, Wang X. Reliability and safety analysis of two modes of dual module hot spare architecture. *J. China Railw. Soc.* 2000; 22(3): 124–127.
19. Wen J, Su H, Shen Q. Reliability and security analysis on two railway signal dual computer hot standby systems. *Railw. Stand. Des.* 2015; 59(3): 110–113.

20. Liu F, Wang H. Comparison of the performance of double 2-vote-2 computer-based interlocking system and double hot standby computer-based interlocking system. *Railw. Signal. Commun.* 2008; 44(2): 26–29.
21. Li J, Zhang Y. Research on safety and performance analysis of computer based interlocking system based on dynamic fault tree analysis. *J. Railw. Sci. Eng*. 2019; 16(6): 1543–1552.
22. Chen G, Fan D, Wei Z, Fang Y. All electronic computer interlocking system based on double 2-vote-2. *China Railw. Sci.* 2010; 31(4): 138–144.
23. Ghadhab M, Junges S, Katoen JP, Kuntz M, Volk M. Safety analysis for vehicle guidance systems with dynamic fault trees. *Reliab. Eng. Syst. Saf.* 2019; 186: 37–50.
24. Dugan JB, Bavuso SJ, Boyd MA. Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Trans. Reliab.* 1992; 41(3): 363–377.
25. Dugan JB, Sullivan KJ, Coppit D. Developing a low-cost high-quality software tool for dynamic fault-tree analysis. *IEEE Trans. Reliab.* 2000; 49(1): 49–59.
26. Abdo H, Flaus JM. Monte Carlo simulation to solve fuzzy dynamic fault tree. *IFAC-PapersOnLine* 2016; 49(12): 1886–1891.
27. Zhu P, Han J, Liu L, Lombardi F. A stochastic approach for the analysis of dynamic fault trees with spare gates under probabilistic common cause failures. *IEEE Trans. Reliab.* 2015; 64(3): 878–892.
28. Ruijters E, Stoelinga M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Comput. Sci. Rev.* 2015; 15: 29–62.
29. Stamatelatos M, Vesely W, Dugan J, Fragola J, Minarick J, Railsback J. Fault tree handbook with aerospace applications. 2002.
30. Faulin J, Juan AA, Alsina SSM, Ramirez-Marquez JE. *Simulation methods for reliability and availability of complex systems*. Springer Science & Business Media . 2010.
31. Zadeh LA. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets Syst.* 1978; 1(1): 3–28.
32. Liang GS, Wang MJJ. Fuzzy fault-tree analysis using failure possibility. *Microelectron. Reliab.* 1993; 33(4): 583–597.

How to cite this article: Yan L, Zhang T, Gao Y, Wang R, and Ding S (2021), Reliability analysis of station autonomous computer system based on fuzzy dynamic fault tree and Markov model, *Engineering Reports*. *2021;00:1–6*.